REMARKS

Claims 1-13, 15-18, and 21-28 are pending. Claims 14, 19, and 20 are canceled herewith.

In an Official Action dated July 17, 2007, claims 14 and 20 were rejected under 35 U.S.C. § 101. Claims 1, 2, 7-9, 14, and 24-26 were rejected under 35 U.S.C. § 102, and claims 3-6, 10-13, 15-23, and 27-28 were rejected under 35 U.S.C. § 103. The rejections are addressed in turn below.

Interview Summary

Applicants would like to thank the Examiner for the courtesy of a telephonic interview on Sep. 27, 2007. At the interview, the undersigned and Examiner Perungavoor discussed the differences between an "encryption algorithm" and a "protocol" or "authentication protocol." Applicants agreed to prepare and submit this written response for the Examiner's further consideration.

Rejection of Claims 14 and 20 Under 35 U.S.C. § 101

Claims 14 and 20 are canceled herewith.

Rejection of Claims 1, 2, 7-9, 14, and 24-26 Under 35 U.S.C. § 102

Claims 1, 2, 7-9, 14, and 24-26 were rejected under 35 U.S.C. § 102(b) as allegedly anticipated by RFC 3244-Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols. The rejections are respectfully traversed.

Independent claims 1, 8, and 24 each contain at least one limitation that is not taught or suggested by RFC 3244, as discussed below. Claims 2, 7, 9, 25 and 26 depend directly or indirectly from claims 1, 8, and 24 and therefore also define over RFC 3244. Claim 14 is canceled.

The at least one limitation in independent claims 1, 8, and 24 that is not found in RFC 3244 is the "encryption algorithm negotiation request" recited in claims 1 and 8 and the "negotiation request" of claim 24. Referring to Applicants' specification, paragraph 0058:

> Next, step 402 shows that computer A can send the encrypted data, along with a negotiation request, to Computer B. A negotiation request can be any piece

or configuration of data that indicates to computer B that Computer A is
prepared to change from one or more first encryption algorithms to one or
more second encryption algorithms. The negotiation request indicates to the
server computer that Computer A supports the requested encryption
algorithm. In the example of Fig. 4, Computer A sends a request to change
from encryption algorithm 1 to encryption algorithm 2. Encryption algorithm
2 may also be referred to as the new encryption algorithm. AES is the new
standard encryption algorithm adopted by the United States Government, and
it is considered likely that AES would be the encryption algorithm 2, though
this choice is not necessary to practice the invention.

(emphasis added).

While RFC 3244 provides change password / set password *protocols*, and supplies a

protocol version number, as noted in the Official Action item 5, a *protocol* as disclosed in the

reference is quite different from an *encryption algorithm* as recited in Applicants' claims.

Examples of encryption algorithms are Ron's Code 4 ("RC4"), Data Encryption

Standard ("DES"), Triple DES ("3DES"), and Advanced Encryption Standard ("AES"). See

Applicants' specification paragraph 0003.

In contrast, a protocol as the term is used in RFC 3244 appears to define the data that

is passed back and forth between client and service when a new password or changed

password is requested. See RFC 3244 Introduction. While some of this data is encrypted, e.g.,

referring to the top paragraph of page 3 of the reference which refers to decrypting a new

password, there is no teaching or suggestion that the encryption algorithm used for such

encryption / decryption is in any way negotiated using a negotiation request. Instead, it

appears to be assumed that both client and server are preconfigured to use a same encryption

algorithm – Applicants make this assumption because there is no discussion of the topic

whatsoever in the reference. In any event, any reference to an encryption algorithm of any

kind is completely absent from RFC 3244. Therefore the notion of an encryption algorithm

negotiation request is beyond the teachings of the reference.

Also, Applicants point out that while a "password" as disclosed in the reference may

define or be utilized to generate and encryption *key*, an encryption *key* is quite different from

an encryption *algorithm*, as explained for example in Applicants' specification paragraph

0004. Therefore, even if RFC 3244 is considered to teach an encryption *key* negotiation

request, this would be quite different from the claimed encryption *algorithm* negotiation

request.

Rejection of Claims 3-6, 10-13, 15-23, and 27-28 Under 35 U.S.C. § 103

Claims 3-6, 10-13, 15-23, and 27-28 were rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over RFC 3244 in view of rpcsec_gss, kadmin service principal (Coffman). While the Official Action admits that RFC 3244 does not disclose all the elements of claims 3-6, 10-13, 15-23, and 27-28, it is alleged that Coffman cures this deficiency. The rejections are respectfully traversed for the reasons provided below.

Independent claims 1, 8, 15, and 24 each contain at least one limitation that is not taught or suggested by RFC 3244 alone or in combination with Coffman. Claims 3-6, 10-13, 16-18, 21-23, and 27-28 depend directly or indirectly from claims 1, 8, 15, and 24 and therefore also define over the combination of references. Claims 19 and 20 are canceled.

The rejections are respectfully traversed for the same reason provided above with regard to the rejection of 1, 2, 7-9, 14, and 24-26. That is, independent claims 1, 8, 15, and 24 each recite an "encryption algorithm negotiation request" or "negotiation request." Like RFC 3244, Coffman is devoid of any reference to an encryption algorithm of any kind. Therefore the reference also cannot and does not teach or suggest an encryption algorithm negotiation request.

Reconsideration and withdrawal of the outstanding rejections is respectfully requested.

Date: October 17, 2007   /Nathaniel Gilder/
                                                    Nathaniel Gilder
                                                    Registration No. 53,233

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439